ELEMENTARY NUMBER THEORY

HOMEWORK 4

(1) Select two random primes p, q of about 10 to 20 digits, form $N = pq$, select e coprime to $(p-1)(q-1)$, and send the pair (N, e) to another student in class; similarly, he will send you his pair.

Now exchange messages using RSA. Write down the encrypted messages c you receive, compute an inverse d of e mod $(p-1)(q-1)$ from a Bezout representation, and decode the messages.

You will need pari for this task. For choosing a 11-digit prime, pick a 11-digit random number like 123456789010 (of coourse this is not random - I'm merely illustrating the idea) and then type `p=nextprime(123456789010)` into `pari`. The answer will be $p = 12345678923$. Pick q, and try a few random values e (they need to be odd – why?) coprime to $(p-1)(q-1)$; you can check this by typing in `gcd(e,(p-1)*(q-1))`.

After you've sent off (N, e), compute a Bezout representation with
`bezout(e,(p-1)*(q-1))`;
to understand the output, type in `?bezout`. Make sure that d is positive; if not, replace it by $d + (p-1)(q-1)$.

Finally, computing powers modulo N is done via

```
c = Mod(m,N)^e
```

If you type in

```
c = Mod(m^e,N)
```

instead, you will get the same result or an error message, depending on the size of e. Can you explain this?

Please hand in your solution either by printing it or by sending it as an email; do not copy the numbers by hand from pari.

If you start pari and do a calculation, you can copy the content of the window into a text file or an email by right-clicking the blue frame at the top and then choosing edit and mark. Then use the arrow and left-clicks to highlight the portion you want to copy, and press enter. Then copy the content to your files. It also works backwards, i.e., you can copy things from a text file into the pari window.

(2) (From the first round of the German mathematical olympiad 2006; it is the traditionally "easy" first problem).

Find two consecutive integers with the property that the sum of their digits is each divisible by 2006.

(3) Consider the password $P = 768462011$, and consider the moduli $n_1 = 919$, $n_2 = 929$, $n_3 = 937$, $n_4 = 941$, and $n_5 = 947$ (these are all primes $> \sqrt[3]{P}$).
   (a) Compute $p_i \equiv P \bmod n_i$ with $0 < p_i < n_i$ for $i = 1, \ldots, 5$.
   (b) Solve the system $x \equiv p_i \bmod n_i$ for $i = 1, 2, 3$ using the Chinese remainder theorem (find the Bezout presentations and follow the notes; first solve the first two congruences, then combine it with the third) and check that the smallest positive solution is $x = P$ (feel free to use pari – this is what it's good for).
   (c) Do the same for the system $x \equiv p_i \bmod n_i$ for $i = 2, 3, 5$.

(4) Find all integers with $\phi(m) = 6$.

(5) Show that if g is a primitive root modulo m, then g is a primitive root modulo any n with $n \mid m$.

(6) (Also from the first round of the German mathematical olympiad 2006): Solve the diophantine equation $x^3 + y^3 = 4(x^2y + xy^2) + 1$. Hint: factor the expression inside the brackets.